

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-251155
(43)Date of publication of application : 27.09.1996

(51)Int.CL

H04L 9/06
H04L 9/14
G09C 1/00

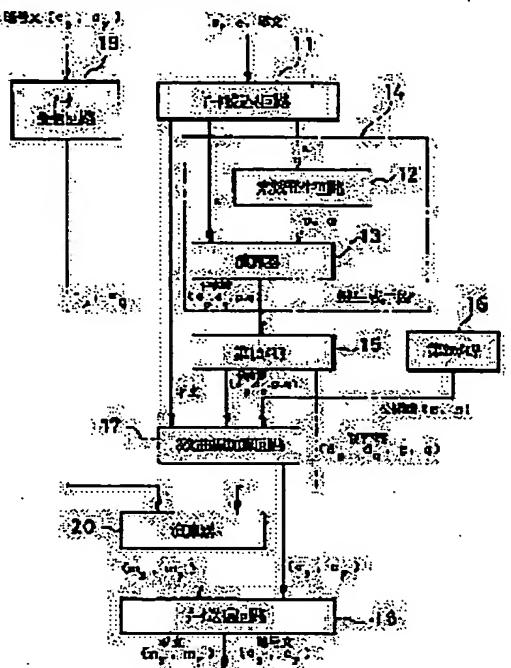
(21)Application number : 07-048575
(22)Date of filing : 08.03.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KOYAMA KENJI

(54) CIPHERING DEVICE, DECIPIHERING DEVICE, CIPHERING AND DECIPIHERING DEVICE AND CIPHER SYSTEM

(57)Abstract:

PURPOSE: To provide a ciphering device and a cipher system particularly excellent in the deciphering speed as compared with RSA ciphers in use.
CONSTITUTION: This device is provided with a key generation means 14 which generates primes p and q and at the time of computation with dp and dq satisfying $dp \equiv 1/e \pmod{p-1}$, $dq \equiv 1/e \pmod{q-1}$, where an integer e is mutually prime with the least common multiple of the product $n=pq$, $(p-1)$ and $(q-1)$, sets the product n and an integer e to be public keys and sets the primes p, q and dp, dq to be secret keys. In addition the device is provided with a ciphering calculation means which makes an integer pair of inputted plain texts correspond to a point on a cubic curve, determines a point obtained by e-folding the point by the use of the public keys by arithmetic on the cubic curve, and outputs arithmetic results as a cipher text, and a deciphering arithmetic means which subjects the integer pair of the inputted cipher text to homomorphic transformation, then raises the result to the dp-th power under a divisor p and dq-th power under a divisor q, and synthesizes them by the use of the Chinese remainder theorem to output a plain text.



LEGAL STATUS

[Date of request for examination] 08.03.1995
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2624634
[Date of registration] 11.04.1997
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Japanese Publication for Unexamined Patent Application

No. 8-251155/1996 (Tokukaihei 8-251155)

A. Relevance of the above-identified Document

This document has relevance to claims 1, 2, and 6 to 13 of the present application.

B. Translation of the Relevant Passages of the Document

See the attached English Abstract.

(5)

送信する場合は、利用者Aは通信線2.4を通じてセンタ

装置2.3から、利用者Bの公用端子n2, e2を受け取
り、前述した如1の実施例で示されるアルゴリズムに従
って暗号化し、その暗号文の密数対を送信回路1.8を通
じて通信線2.8へ送出する。

[0024] 利用者Bの暗号装置1.9に受信された暗号文は、前記の通り復
号化されて、元の平文が位元される。利用者Bから利用
者Aへの暗号通信も同様に行なわれ、この場合は鍵
n1, e1, d1, p, qが用いられる。

[0025] 以上説明したように本実施例は、次の長所
をもつている。

(1) 本実施例の暗号方式は従来のRSA暗号に比べ
て、復号化速度が約2倍であり、暗号化速度はほぼ同じ
である。RSA暗号は通常、復号に時間がかかつていた
ので、本実施例の方式では全体の速度向上が約2倍とな
っている。

(2) 本実施例の暗号方式はRSA暗号と同じレベルの
安全性をもつ。

[0026]

【発明の効果】 以上説明したように本実施例は、従来のR
SA暗号に比べたとき、復号化速度が約2倍と高速であ
りながら、暗号化速度及び安全性はほぼ同じであるとい

う優れた効果を備える。

【画面の簡単な説明】

【図1】 本発明に係る暗号装置の一実施例の構成
を示すブロック図である。

【図2】 本発明に係る暗号システムの一実施例を示すブ
ロック図である。

【符号の説明】

1.1 データ読み込み回路
1.2 密数生成回路
1.3 演算器
1.4 関生成手段
1.5 第1のメモリ
1.6 第2のメモリ
1.7 3次曲線加算回路
1.8 データ送信回路
1.9 データ受信回路
2.0 比較器

2.1 暗号装置
2.2 明号装置
2.3 センタ装置

11

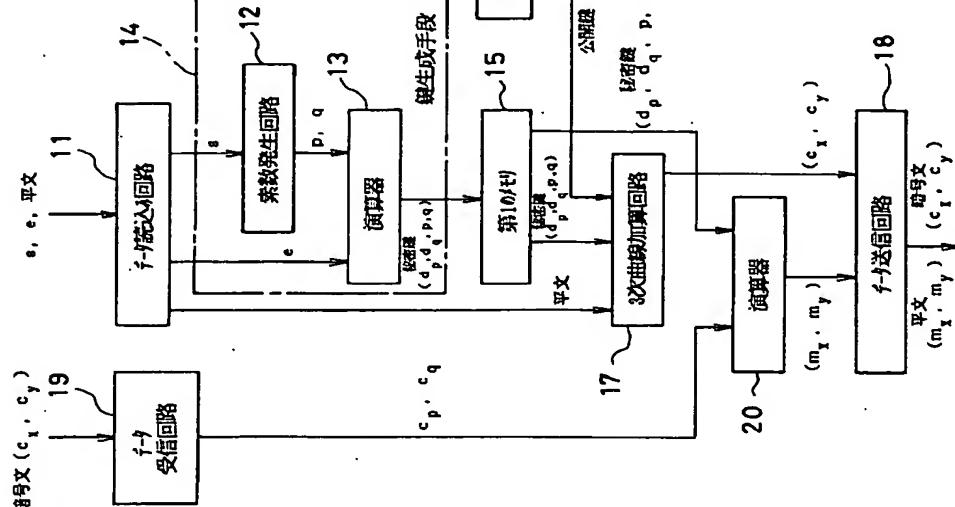
2.4, 2.5, 2.8 通信線

2.6 送信回路

2.7 鍵ファイル

(6)

【図1】



(7)

